UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/565,571	08/02/2006	Estelle Transy	18394017US1RVLPA61423US	2383

26221 7590 02/19/2010

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
02/19/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	10/565,571	TRANSY ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *21-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *21-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to action filed.11/30/2009. Claims 21, 25, 27, and 29 amended. Claims 21-31 are pending,

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 21, 25, 27, and 29 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The Examiner respectfully submits applicant's newly amended claim subject matter of "wherein the distinct set of data comprises a first password for the first entity and a second password for the second entity" lacks support of applicant's original specification. Applicant recites the following in paragraph 61: "a user name "User-Name" attribute identical to the two concatenated identifiers ID1|ID2, a password "CHAP-Password" attribute identical to the two concatenated passwords AUTH1|AUTH2, as well as a "CHAP-Challenge" attribute intended to receive the random number RAND used to generate the passwords, wherein the number RAND is determined by the specialized server on the basis of an identifier of the connection session in progress with the terminal". It would appear to one

of ordinary skill in the art that two the concatenated passwords as recited in paragraph 61 are associated with a single user and not two individual users as claimed.

Additionally, applicant's newly amended subject matter of a "first user identifier" and a "second user identifier" lacks support of applicant's original disclosure. As recited in paragraph 61 of applicant's original specification, ID1 and ID2 are associated with identifying one user. This fact is also recited in paragraph 64 of applicant's original disclosure as well.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 21-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Chaudhary et al. (US Patent No. 7,155,526 and Chaudhary hereinafter).

4. As to claim 21, Chaudhary teaches a method for authenticating a user (e.g., customer) for access to at least two entities of a data transmission network via a terminal, each data entity having an associated authentication device (i.e., ...teaches sending information to negotiate authentication and other network configuration needed

to make communication [col. 9, lines 15-25]), the authentication devices being independent of each other (i.e., ...teaches a RLM forwards authentication messages from the MLC to the RAC. The RAC provides protocol stacks and interworking functions in order to allow the MLC to talk to a Home Location Register (HLR), which is a standard network element in the GSM core network that handles authentication. After the customer is authenticated, the RLM and the MLC set up a "tunnel" employing Point-to-Point Protocol (PPP) Over Ethernet (PPPOE), and all of the data packets received on this tunnel are forwarded by the RLM to the Gateway GPRS Support Node (GGSN), a standard network element in the GSM/GPRS network that provides interconnection to the Internet or other packet data network [col. 3, lines 45-60]), the method comprising: -

a random number (e.g., RND) is transmitted to the terminal [503, fig. 5],

- a distinct set of data for each of a first entity and a second entity for authenticating the user to both the two first and the second entities of the network is calculated using at least one predefined cryptographic algorithm applied to the random number received and at least one secret key specific to the user (i.e., ... teaches sending an Authentication Request packet 516 including the Kc, a key generated by secret parameters known only to the HLR and the SIM card, using A8 type GSM authentication protocols and one or more RANDs, a random number of 64 bits, and the Signed Response (SRES) that can be authenticated using A5 type authentication protocols, which proves that the HLR knows the secret shared with the SIM card and is used to provide authentication of the SIM card to the operator's network [col. 10, lines 20-35]), wherein the distinct set of data comprises (i) a first password for the first entity

and (ii) a second password for the second entity, the terminal inserts, in an access request (i.e., ..teaches sending one or more RANDs, a random number of 64 bits [col. 10, lines 20-35]),

first user identifier data and second user identifier data for identifying the user to said two first and second entities of the network and the two distinct sets of data (i.e., ..teaches the User equipment uses unique identifiers [col. 9, lines 30-40]), the terminal transmits the access request to an access controller (i.e., ...teaches transmitting a access request [501, 502, 515, Fig. 5]), wherein the inserted data for authenticating the user comprises a distinct set of data for the first and second two entities [501, Fig. 5]),

- the access controller transmits, to each of the authentication devices for the two first and second entities, a respective authentication request containing the first user identifier data and the first password for the first entity [502, 515, fig, 5]),

identification data and (ii) the second use identifier data and the second password for the second entity (i.e., ...teaches sending an Authentication Request packet 516 including the Kc, a key generated by secret parameters known only to the HLR and the SIM card, using A8 type GSM authentication protocols and one or more RANDs, a random number of 64 bits [col. 10, lines 20-35]), the distinct set of inserted data for authenticating the user to the respective entity of the network contained in the access request (i.e., ...teaches sending information to negotiate authentication and other network configuration needed to make communication [col. 9, lines 15-25]), the authentication devices of the entities each carry out a user authentication procedure [fig. 5], on the basis of the user identification identifier data and the respective distinct set of

authentication data transmitted to the respective authentication device (505, fig. 5), contained in the authentication requests, and authentication reports containing results of the authentication procedures carried out by the authentication devices of each of said two first and second network entities are transmitted to the terminal (i.e., ...teaches sending authentication status message [510, fig. 5]).

5. As to claim 22, Chaudhary teaches a method characterized in that it includes a preliminary step in which the terminal establishes a connection with a specialized server via the network, wherein the random number is generated and transmitted to the terminal by the specialized server when the connection has been established (i.e., ...teaches sending an Authentication Request packet 516 including a GSM authentication protocols and one or more RANDs, a random number of 64 bits [col. 10, lines 20-35]).

6. As to claim 23, Chaudhary teaches a method characterized in that the access request transmitted by the terminal is transmitted to the specialized server which inserts therein the random number used to calculate the authentication data [516, fig. 5}, the access request is then transmitted to the access controller which inserts the random number into the authentication requests transmitted to the authentication devices for the two entities [503, 516 fig. 5}.

7. As to claim 24, Chaudhary teaches a method characterized in that the identification data inserted into the access request is in the form: "IdA@DomainA" in which: - "IDA" represents the identifier for identifying the user to the network entity, - "DomainA" represents the identifier of the network entity in the network, with the access controller determining the entities to whom the authentication requests will be transmitted on the basis of the "DomainA" identifiers of the network entity contained in the access request (i.e., ...teaches the using a domain name service query for the purpose of determining how the packet information will be routed [column col.7 , lines 45-55]).

8. As to claim 25, Chaudhary teaches a user terminal capable of accessing, via the access network (530, fig. 5), at least a first entity and a second entity two connected to a data transmission network (fig. 50, each data entity having an associated authentication device [fig. 2], the authentication devices being independent of each other:

characterized in that it includes: a transmitting apparatus that transmits access requests to the authentication devices for the first and second at least two entities of the network (i.e., ...teachs RLM for transmitting request [521, fig. 5]), which requests contain data for identifying and authenticating the user to first and second network entities and each request including user identifier data and a distinct set of data comprising (i) a first password for the first entity and (ii) a second password for the second entity; a receiving apparatus that receives a random number when a connection with the network is

established, a cryptographic calculating apparatus that applies at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to the first and the second entities of the network (i.e., ... teaches sending an Authentication Request packet 516 including the Kc, a key generated by secret parameters known only to the HLR and the SIM card, using A8 type GSM authentication protocols and one or more RANDs, a random number of 64 bits, and the Signed Response (SRES) that can be authenticated using A5 type authentication protocols, which proves that the HLR knows the secret shared with the SIM card and is used to provide authentication of the SIM card to the operator's network [col. 10, lines 20-35]), and inserting apparatus that inserts, into each transmitted access request, first user identifier data and second user identifier data for identifying the user to said first and second e-ash network entities and t-he calculated authentication data (i.e., .teaches the inclusion of a user identifier [502, fig. 5]), wherein the calculated authentication data comprises a distinct set of authentication data for the first and second network entities [col. 10, lines 20-35].

9. As to claim 26, Chaudhary teaches a terminal characterized in that it includes an external module designed to be connected to each of the user terminals and including a receiving apparatus that receives the random number from the terminal to which it is connected, a cryptographic calculation apparatus that executes the predefined cryptographic algorithm based on the random number, and for transmitting, to the terminal, at least one data item for authenticating the user to an entity of the network,

obtained by the cryptographic calculations (i.e., ...teaches during the CHAP exchange the Challenge field data sent to the UE 520 in packet 505 from the RLM 521 consists of two 16 byte random numbers and the MAC_RAND, which is a signed version of the two random numbers combined with the nonce, the two Kcs, the IMSJ, and the two SRESs using the shah-1 algorithm, a hash algorithm. Other hash algorithms, such as MD-5 may also be used. A Kc can be generated by the MLC on the UE 520 from each RAND sent in message 503 to the RLM 521 and forwarded to the UE 520 in the CHAP challenge message 505 by sending each RAND to the SIM card 417 and getting a Kc as the response generated by the GSM algorithm A8 [column 11, lines 30-45]).

10. As to claim 27, Chaudhary teaches a access controller, characterized in that it includes a receiving apparatus that receives a request for access to a first entity and a second entity in a data transmission network coming from a user terminal and transmitted via said network (i.e., discloses the sending a request for access in a data transmission network [fig. 5] The actual network is disclosed in figure 2), an extracting (e.g., discovers) apparatus that extracts, from the access request, user identifier data the data for identifying and authenticating the user to the first and second network entities (i.e., The MLC has registered with the device driver of the WLAN Radio 406 to receive copies of all of these types of packets. The PADO packets contain the IEEE MAC address of the RLMs 206. In this manner, the MLC can discover the address of the RLMs 206. The MLC now uses this address over the bridged networks 214 and 215 and air link 218 in order to set up a PPPOE tunnel between itself and its chosen RLM

206 [col. 8, lines 15-30]) , each network entity having an associated authentication device [fig. 5], the authentication devices being independent of each other [fig. 5], wherein the data for authenticating the user to at least the first and second network entities comprises a distinct set of data for each of the network entities, the distinct set of data comprising (i) a first password for the first entity and (ii) a second password for the second entity, transmitting apparatus that transmits, to each of the authentication devices for the first and second entities, a respective authentication request containing the user identifier data for identifying and authenticating the user to a respective one first and second network entity contained in the access request (i.e., ... teaches sending an Authentication Request packet 516 including the Kc, a key generated by secret parameters known only to the HLR and the SIM card, using A8 type GSM authentication protocols and one or more RANDs, a random number of 64 bits, and the Signed Response (SRES) that can be authenticated using A5 type authentication protocols, which proves that the HLR knows the secret shared with the SIM card and is used to provide authentication of the SIM card to the operator's network [col. 10, lines 20-35]).

11. As to claim 28, Chaudhary teaches a access controller characterized in that it also includes a receiving apparatus that receives user authentication reports (i.e., ...teaches sending authentication status [510, fig. 5]), transmitted by the entities in response to the authentication requests [508, fig. 5]), and a transmitting apparatus that transmits, to the user terminal, and authentication report based on the reports received from the entities [510, fig. 5]).

12. As to claim 29, Chaudhary teaches a system for authenticating a user in an attempt to access at least two entities of a data transmission network to which network entities are connected [fig. 5 & fig. 2], and which user terminals can access via access networks, characterized in that it includes: - a user terminal (e.g., user equipment) characterized in that it includes [520, fig. 5]: - a transmitting apparatus that transmits access requests to an entity of the network [502, fig. 5], which requests contain first user identifier data and second user identifier data for identifying and authenticating the user to first and second entities of the network (515, fig. 5);

and a receiving apparatus that receives a random number when a connection with the network is established (503, fig. 5), a cryptographic calculating apparatus that applies at least one predefined cryptographic algorithm to the random number received so as to obtain data for authenticating the user to at least two entities of the network (i.e., ...teaches during the CHAP exchange the Challenge field data sent to the UE 520 in packet 505 from the RLM 521 consists of two 16 byte random numbers and the MAC_RAND, which is a signed version of the two random numbers combined with the nonce, the two Kcs, the IMSJ, and the two SRESs using the shah-1 algorithm, a hash algorithm. Other hash algorithms, such as MD-5 may also be used. A Kc can be generated by the MLC on the UE 520 from each RAND sent in message 503 to the RLM 521 and forwarded to the UE 520 in the CHAP challenge message 505 by sending each RAND to the SIM card 417 and getting a Kc as the response generated by the GSM algorithm A8 [column 11, lines 30-45]), and an inserting apparatus that inserts,

into each transmitted access request, first user identifier data and second user identifier data and a distinct set of data for each of the first entity and the second entity, wherein the distinct set of data comprises (i) a first password (e.g. random number) for the first entity and (ii) a second password (e.g. random number) for the second entity a distinct set at least one authentication server for each of the two network entities, designed to identify and authenticate the users on the basis of the user identifier data and the respective distinct set of identification and data transmitted to each respective authentication device, the authentication devices being independent of each other (i.e., ...teaches sending an Authentication Request packet 516 including the Kc, a key generated by secret parameters known only to the HLR and the SIM card, using A8 type GSM authentication protocols and one or more RANDs, a random number of 64 bits [col. 10, lines 20-35]), the distinct set of inserted data for authenticating the user to the respective entity of the network contained in the access request (i.e., ...teaches sending information to negotiate authentication and other network configuration needed to make communication [col. 9, lines 15-25]);

- an access controller characterized in that it includes a receiving apparatus that receives requests for access to at least two entities of the data transmission network coming from user terminals and transmitted via said network [521, fig. 5], an extracting apparatus that extracts, from each of the access requests, the data for identifying and authenticating the user to at least two network entities (i.e., ...teaches using the data sent over in the request for purposes of authentication [516, fig. 5]], a transmitting apparatus that transmits, to each of the two entities, a respective authentication request

containing the data for identifying and authenticating the user to the two entities, contained in the access request (i.e., ..teaches data transmission within a communication network of multiple communicating entities [fig. 5 & fig. 2]).

13. As to claim 30, Chaudhary teaches a system characterized in that it also includes a specialized server connected to the network so as to be connected to the user terminals when a connection has been established between the terminal and the network [521, fig. 5], wherein the specialized server includes a generating and transmitting apparatus that generates and transmits a random number to each of the terminals with which a connection is established, and an inserting apparatus that inserts the random number into each of the access requests transmitted by the terminals [503, fig. 5] .

14. As to claim 31, Chaudhary teaches a system characterized in that each entity of the network includes a storing apparatus that stores secret keys of users (i.e., ...teaches including the Kc, a key generated by secret parameters [column 10, lines 20-35]), a determining apparatus that determines the data for authenticating the user to the entity by applying the predefined algorithm to the random number received in a authentication request and to the secret user key, and that compares the result obtained to the user authentication data received in the authentication request [505, fig. 5], wherein the user is properly authenticated by the entity only if the result of the

cryptographic calculation obtained is identical to the authentication data contained in the authentication request [column 11, lines 30-45].

Response to Arguments

Applicant's arguments with respect to claims 21-31 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431